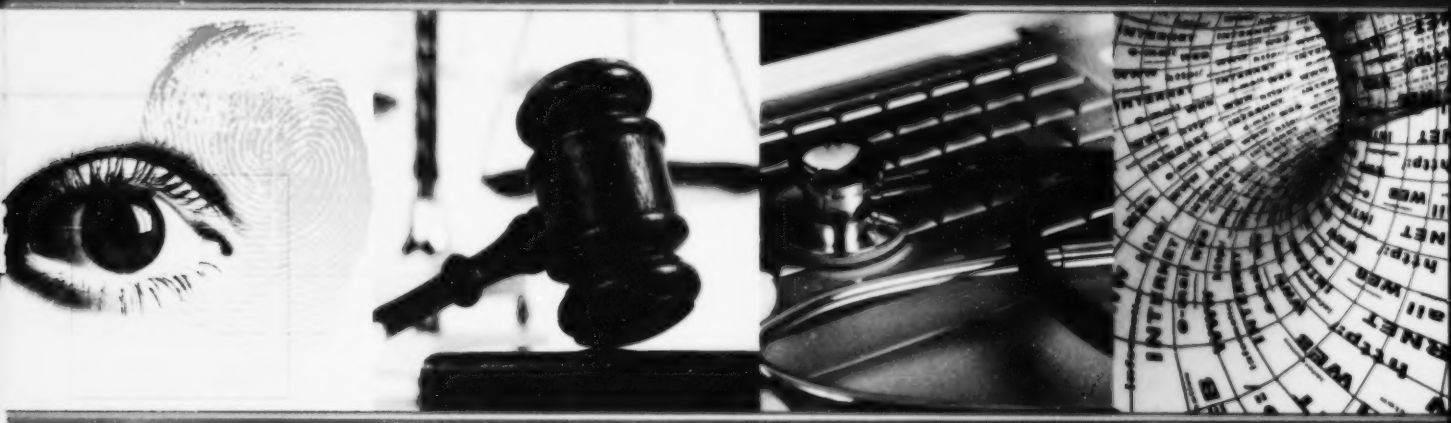


ACCESS & PRIVACY

A TIME FOR INNOVATION

INFORMATION & PRIVACY COMMISSIONER OF ONTARIO
2009 ANNUAL REPORT

Information and Privacy
Commissioner/Ontario
Commissaire à l'information
et à la protection de la vie privée/Ontario

May 11, 2010

The Honourable Steve Peters, MPP
Speaker of the Legislative Assembly of Ontario

I have the honour to present the 2009 Annual Report of the Information and Privacy Commissioner of Ontario to the Legislative Assembly.

This report covers the period from January 1, 2009 to December 31, 2009.

Please note that additional reporting from 2009, including the full array of statistics, analysis, video commentary and supporting documents, may be found within our online Annual Report section at www.ipc.on.ca.

Sincerely yours,

Ann Cavoukian, Ph.D.
Commissioner

Enclosure

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

2, rue Bloor est
Bureau 1400
Toronto (Ontario)
M4W 1A8

416 326 3333
1 800 387 0073
Fax/Télec: 416 325 9195
TTY: 416 325 9539
http://www.ipc.on.ca

Commissioner's Message
2009: A Year of Innovation

Ann Cavoukian, Ph.D.
Information & Privacy Commissioner,
Ontario, Canada

2009 PROVED TO BE A YEAR THAT REQUIRED INNOVATION TO MEET INCREASINGLY NEW CHALLENGES. I have fashioned a particular philosophy for my office known as the 3Cs: Move forward by way of Consultation; Collaboration; and Co-operation. In 2009, we fully embraced that philosophy — finding better ways of working with organizations in order to generate practical, workable solutions to privacy and access issues. I am particularly proud of the innovation and sheer commitment displayed by my office — as evidenced by our probe into jury vetting in 2009 (see following page).

In a further innovation, we are now publishing the majority of our Annual Report content online (www.ipc.on.ca). This not only allows us to include more supporting documents and information, but it is also cost-effective and more environmentally friendly.

Challenges for a Third Term

I was deeply honoured when the Legislature of Ontario reappointed me in May 2009 to serve as the province's Information and Privacy Commissioner for a third term. I am grateful to the members of the legislature for their strong support.

After my first reappointment in 2004, I said that we were in the midst of profound change in the areas of privacy protection and access to government information. Since that time, the pace has grown exponentially.

Privacy by Design

In this age of massive electronic information storage, privacy challenges expand and modify daily. To meet these challenges head-on, I intend to advance the benefits of *Privacy by Design (PbD)*. Developed here in Ontario, *PbD* encapsulates a proactive approach to privacy. With *PbD*, privacy is embedded as the *default* in the design of technology, business practices and physical design/infrastructure — as opposed to privacy being bolted on as an afterthought. I challenge all organizations that connect with personal data to meet the gold standard we have created for privacy: *Privacy by Design*. *See Key Issue on page 7.*

Privacy-protective electronic health records

I remain committed to working with health-care stakeholders to help bring about effective and privacy-protective electronic health record systems. Electronic systems offer many benefits to both practitioners and patients — including improved clinical decision-making, greater patient access to their records; and more effective diagnosis and treatment — but the potential risks to privacy must be minimized during the design and implementation of these systems.

Access by Design

I will continue to make "transparent and accountable government" a key emphasis, and will strongly urge both provincial and local governments to develop proactive disclosure programs under which general records — ranging from agendas to expense accounts to contract disclosures — are routinely disclosed using websites and other communications technologies. *See Key Issue on page 7.*

More organizations under FOI

In my 2004 Annual Report, I urged the Ontario government to compile and review institutions that are primarily funded by government but not yet covered by the *Acts*. One of the foundations underlying FOI is the principle that organizations that exist by virtue of public funding should be subject to public scrutiny through FOI laws. Universities were added under the *Freedom of Information and Protection of Privacy Act* in 2006. Now, the Ontario Hospital Association has asked the province to place Ontario hospitals under the *Act*. While these represent important steps, more can be done. *See my Recommendation on page 8.*

Innovative Approach to Investigations

My office has made great strides in honing its methods for conducting privacy investigations.

In 2009, one province-wide privacy investigation was particularly challenging. This Commissioner-initiated investigation was launched to determine whether the privacy rights of prospective jurors had been breached when various police forces used confidential databases and other methods to selectively probe the background of potential jurors, on behalf of certain Crown attorneys. Due to the potentially far-reaching implications of this investigation, we developed even more sophisticated and innovative investigative techniques.

Commissioner Cavoukian is flanked by Assistant Commissioners Ken Anderson (L) and Brian Beamish (R) as she outlines her special investigation report on juror vetting in a packed Queen's Park media studio.

Here's why I took such action. At the outset, there were reports in the media suggesting that, due to a lack of subpoena-making power, my Office's investigation would not be very effective. To counter such concerns, I took special steps to ensure that our investigation would be thorough and comprehensive. We began by asking the Ministry of the Attorney General (MAG) to issue a directive that all electronic and paper documents related to

jurors be preserved. IPC staff then conducted site visits in seven municipalities across the province, conducting numerous face-to-face interviews with Crown attorneys, court staff, police officials, defence counsel and others with knowledge of jury vetting processes. Although these visits provided invaluable information, in order to verify how widespread jury practices were, we needed to break new ground.

First, we developed and administered a detailed survey to all 55 Crown attorney offices in Ontario — a survey that would be backed up with sworn affidavits by senior officials. The survey asked each of the 55 offices to provide the IPC with information about their past practices with respect to background checks on prospective jurors. Along with their completed survey, each office was asked to provide the IPC with all jury lists that had been used by that office since 2006. Since the scrutiny of actual jury lists was the best way to determine whether the lists had been vetted, this step helped to verify the answers provided by each Crown attorney office. Additionally, I went further by seeking out the assistance of staff from the Auditor General's office to verify the document capture process. I also took an unprecedented step — requiring sworn affidavits from the seven Regional Crown attorneys and the Assistant Deputy Crown attorney responsible for prosecutions. The purpose of these affidavits was to verify that the answers provided on the surveys were complete and accurate, and that my office had been provided with all existing jury lists.

The methodology developed during this investigation proved to be very successful, resulting in a thorough and comprehensive order — one that provided the impetus for a fundamental shift in the manner in which prospective jurors are screened in Ontario.

In my order, *PO-2826, Excessive Background Checks Conducted on Prospective Jurors: A Special Investigation Report*, I recommended that screening practices be centralized — that MAG, through its Provincial Jury Centre (PJC), be the only body to screen jurors, instead of the existing 55 district offices. Since the PJC already possesses the names and personal information of all prospective jurors, it was a logical choice to assume this responsibility. As the single entity operating from a single location, the PJC would be able to implement strict privacy and security measures consistently — ones that can be strongly enforced.

I am happy to report that my order and all of the recommendations made have been accepted and are being implemented in appropriate phases.

A Year of Being Proactive

SmartPrivacy for the Smart Grid

The smartening of our electricity grid will offer many benefits for the economy and the environment — but we must make sure that consumer privacy is not sacrificed amidst a sea of enthusiasm for electricity reform. My overarching privacy concern is the Smart Grid's ability to greatly increase the amount of information that is currently available relating to the activities of individuals within their homes — their habits and behaviours. In response, I issued the publication, *SmartPrivacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation*. In 2009, the IPC was extensively involved in advancing privacy on the Smart Grid, meeting with local electricity distributors and government officials to ensure that Ontario plays a leading role in this area. *See my Recommendation on page 9.*

Home Health Care

Given the demographics of our aging population, the demand for remote home health technologies will continue to rise. Advances in connectivity, sensor technology and computing power will deliver innovative, long-term health-care services in the future. However, technology developers must understand that system functionality ***and*** privacy of the individual must both be delivered in unison. Our work in this area in 2009 culminated with a joint publication with Intel and GE Healthcare on the subject: *Remote Home Health Care Technologies: How to Ensure Privacy? Build It In:* Privacy by Design.

Ongoing Support for IPSI — SmartData

Since 2007, I have served as Chair of the Advisory Council for the Identity, Privacy and Security Institute (IPSI) at the University of Toronto — a multi-disciplinary institute that explores the relationship between technology and privacy. In 2009, IPSI's focus was on SmartData — a research program

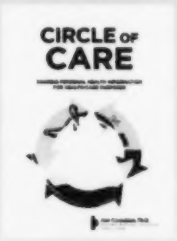
to develop Web-based intelligent agents that will perform two tasks: securely store an individual's personal and/or proprietary data, and protect the privacy and security of the data by only disclosing it in accordance with instructions authorized by the data subject. This has attracted the interest of high profile organizations such as Hewlett-Packard and GS1 Canada who will work with IPSI on the solutions required when personal information and business needs intersect in the 21st century.

Health Care in 2009

PHIPA Seen as the Framework for Revisions to U.S. Legislation

There could have been no better milestone for the fifth anniversary of Ontario's *Personal Health Information Protection Act* (*PHIPA*) than the recognition given it by key U.S. health officials. The U.S. Institute of Medicine's Committee (IOM) on Health Research and the Privacy of Health Information recommended that a new approach be developed towards protecting privacy in health research. I am proud to say that in the IOM's report, the only existing statute they pointed to for the purpose of serving as a viable model for revisions to the *Health Insurance Portability and Accountability Act's* Privacy Rule was Ontario's *PHIPA*. My office was asked in 2009 to join the U.S. National Institutes of Health's efforts to build upon the IOM's report.

Circle of Care



In the autumn of 2009, I issued a new publication entitled *Circle of Care: Sharing Personal Health Information for Health-Care Purposes.* Developed in collaboration with seven health organizations, it was produced to assist health-care workers in clarifying any confusion about when health information custodians could assume a patient's *implied consent* to collect, use or disclose personal health information. The response we have received to this work has been overwhelming, with numerous accolades from health-care workers across the province.

Much Work to Be Done

Just hours before 2009 arrived, records containing personal health information were found scattered on the street outside an Ottawa medical centre housing a medical laboratory. I responded immediately to ensure that the records were secured and then commenced an investigation. It was disheartening to learn that this case was almost identical to my first health order (HO-001) in 2005 regarding an incident in Toronto. As a direct response, I issued a publication in 2009 in collaboration with the National Association for Information Destruction (NAID), *Get rid of it securely to keep it Private: Best Practices for the Secure Destruction of Personal Health Information,* which clearly outlines a number of steps to be employed in the secure destruction of health records.

Just before 2009 came to a close, I experienced another case of déjà vu when I was notified that a USB key lost by Durham Region contained the unencrypted personal health information of almost 84,000 patients who had received H1N1 flu shots. If these records had been encrypted, as I had called for previously, the entire crisis would have been averted. *See Key Issues on page 6.*

My Personal Thanks!

I would like to sincerely thank the staff of my office for their ongoing efforts in a year in which we were able to fulfil and move forward the mandate of this office. The people of Ontario are very fortunate to have such talented and dedicated people working on their behalf — for open government, and for the protection of their privacy. I am now, as always, eternally grateful to you.

Ann Cavoukian, Ph.D.

Information & Privacy Commissioner, Ontario, Canada

ACCESS & PRIVACY

A TIME FOR INNOVATION

Table of Contents

Letter to the Speaker IFC

Commissioner's Message 1

Key Issues 6

- Accountability in Juror Vetting 6
- Safeguarding Personal Information 6
- Privacy by Design 7
- Access by Design 7

Recommendations 8

1. New, innovative framework needed for abandoned records 8
2. More coverage required for greater transparency and accountability 8
3. Ensure privacy is embedded into the Smart Grid 9

Requests by the Public 10

Response Rate Compliance 11

Appeals 12

Privacy 13

The *Personal Health Information Protection Act* (*PHIPA*) 14

Judicial Reviews 16

Financial Statement IBC

Find more resources and full statistics in our online 2009 Annual Report section at www.ipc.on.ca

Key Issues

Accountability in Juror Vetting

Trial by jury is not only a fundamental part of our criminal justice system — it is an integral element of the essential freedoms that form the foundation of democracy. It follows that any practice that taints, or is perceived to taint, the jury process, strikes at the very heart of the values we share as citizens. For these reasons, the IPC's investigation into jury vetting was one of our most significant undertakings in 2009, and in the history of our office.

The IPC investigation team went to great lengths to establish whether the privacy rights of prospective jurors were breached when the police, on behalf of certain Crown attorneys, conducted background checks through a variety of means, ranging from accessing confidential databases, to informally gathering anecdotal information. The key findings of our investigation included:

- One-third, or 18 of the 55 Crown attorney offices in Ontario had received background information about prospective jurors since March 31, 2006;
- All 18 of these Crown attorney offices had gathered personal information that exceeded the criminal conviction eligibility criteria set out in the *Juries Act* and *Criminal Code*; and
- There were varying practices regarding the disclosure of this information by Crown attorney offices to defence counsel.

Along with an Order for Crown attorneys to cease collecting any personal information of potential jurors, beyond that which was sanctioned by the *Juries Act* and *Criminal Code*, the Commissioner paved the way for a fundamental shift in the way that jurors are screened. By the end of 2009, amendments to the *Juries Act* had been passed — enabling the creation of a more privacy-protective centralized jury vetting system, and the introduction of greater accountability into Ontario's criminal justice system.

Safeguarding Personal Information

There were a number of unfortunate reminders in 2009 of the need for organizations to embed privacy controls into their core business practices, to ensure that personal information is managed correctly. In particular, three high-profile cases highlighted why it is crucial for organizations to practice end-to-end data protection.

- Just as 2009 was about to arrive, records containing personal health information were found scattered on the street next to a medical centre housing a medical laboratory in Ottawa;
- In July 2009, Toronto Hydro advised that its e-billing system was breached and that the personal information of some of its customers may have been inappropriately accessed; and
- Just before the year came to close, a USB key containing the health data of almost 84,000 patients who had received H1N1 flu shots in Durham Region, was lost.

In our modern-day world where vast databases of personal information exist, it is absolutely crucial that all organizations, large, medium or small, employ best practices in their information management. This includes "secure destruction," where records containing any personal information are permanently destroyed or erased in an irreversible manner, and that personal information transported on electrical devices be strongly encrypted.

It is a sad fact that the majority of privacy breaches occur largely because of poor information management practices. No longer can organizations ignore the fact that it is they, not individuals, who are responsible for any personal information they collect (even after it has outlived its usefulness) from collection to destruction — end-to-end.

Privacy by Design

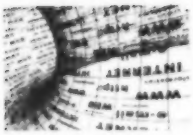
Over the years, a zero-sum paradigm has prevailed — one in which privacy has competed with other values, such as security, in a zero-sum "win-lose" equation. The logic of this flawed approach is that in order to protect ourselves from the threat of terrorism, society must forfeit some measure of privacy. This notion, however, is based on a false dichotomy — that privacy and security are mutually opposing — nothing could be further from the truth.

Privacy *can* and *must* coexist alongside other critical requirements — not only security, but also functionality, efficiency and usability in a doubly-enabling "positive-sum" or "win-win" equation.

This may be accomplished through *Privacy by Design (PbD)* — a concept developed by Commissioner Cavoukian, here in Ontario, back in the '90s. It prescribes that privacy be embedded directly into the design and operation, not only of technology, but also of business processes and physical spaces. Instead of treating privacy as an afterthought — "bolting" it on after the fact — *PbD* is proactive and preventative in nature; an innovative approach sorely needed in today's world of increasingly interconnected technologies and extensive data collection.

Since the personal information of Ontarians is stored globally, protecting their privacy means advancing *PbD* on the world stage. In 2009, the Commissioner finalized *The 7 Foundational Principles of Privacy by Design*, hosted the first PbD Challenge event in Toronto, as well as holding a sold-out international summit of Commissioners and global privacy leaders. To ensure that it continues to gain strong global momentum, she has launched www.privacybydesign.ca as a repository of *PbD* information. The Commissioner will continue to advance *PbD*, for the benefit of the people of Ontario and beyond, throughout her current term.

Access by Design



Government organizations can develop information management practices that go beyond just the basic measures of reactive disclosure. When a government institution sits down to identify exactly how it can make public data more easily accessible, it starts a process that I call, *Access by Design (AbD)*. This includes more than just accountable and transparent government. *AbD* also embraces the concept of a more responsive and efficient government that engages in collaborative relationships with those it serves.

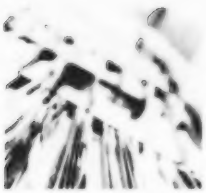
The City of Toronto provides an excellent example of how a government organization can take the proactive approach in disseminating government records. On its website, for example, you can find records of office expenses, salaries and benefits, and information about contracts that have been awarded. In addition, it created a new Web portal in 2009 under the Open Toronto initiative, designed to make city data more accessible.

A number of other local government organizations, including the Region of Waterloo and the Sudbury District Health Unit, publish key information on their websites about such things as restaurant health inspection results. At the provincial level, the Ministry of the Environment has undertaken a number of initiatives to streamline access to public data, from air quality to sport fishing.

Each government organization, at both the provincial and municipal level, should review how effective and efficient it is in releasing the types of information that its citizens are interested in, and have a right to access.

Find more resources related to all of these Key Issues in our online 2009 Annual Report section at www.ipc.on.ca

Recommendations



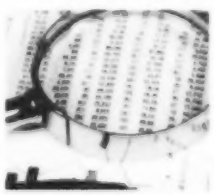
In recent years, my office has investigated numerous instances of personal health information records that have been abandoned by persons or organizations in the health-care field. Typically, this happens when a health-care professional ceases to practice, either because of retirement, moving out of the province, or because he or she has been deemed unfit to practice by their regulatory body. Often, we receive a call from a landlord who is looking to lease the space formerly occupied by the custodian, but needs to deal with the problem of abandoned health records.

In December 2006, I issued Order HO-003 under the *Personal Health Information Protection Act* (*PHIPA*) to a medical and rehabilitation clinic that closed its operations and left behind the health records of many of its clients. This order emphasized that health information custodians are under a continuing obligation to retain, transfer and dispose of health records in a secure manner, including upon the cessation of their practice. The order was accompanied by guidelines and best practices that provided guidance on implementing these requirements. Despite these measures, abandoned health records continue to pose significant risks to the privacy of patients and the delivery of effective health care.

PHIPA has proven ineffective in situations where the custodian is unwilling or unable to meet his or her obligations upon the cessation of their practice, or simply cannot be found. Solutions to this problem have been developed in other jurisdictions. In Alberta, amendments have been passed to the province's *Health Professions Amendment Act* that, once proclaimed, will obligate regulatory colleges to adopt standards of practice requiring their members to make arrangements to ensure that patient records are not abandoned. Should a member, or former member, abandon patient records, the college will have the responsibility to ensure that the records are secured. Further, the amendments will permit a court to order the sheriff to seize abandoned patient records and place them in the custody of a trustee.

A different approach has been adopted in California. Bill AB 1094, which came into effect on January 1, 2010, requires a business to take all reasonable steps to dispose of customer records when those records are no longer required. Disposal must occur through shredding, erasing or otherwise modifying the personal information in the records to make it unreadable through any means. An innovative feature of the bill is a provision that a business, including a storage company or commercial landlord, cannot be the subject of legal action for disposing of abandoned records through the proper means.

Based on my office's experience with *PHIPA*, I believe there is a growing need for Ontario to examine new and innovative approaches to the problem of abandoned health records. I urge the Ministry of Health and Long-Term Care engage in consultations with relevant stakeholders with a view to amending *PHIPA*, and any other relevant legislation, to provide a comprehensive legislative framework to ensure that health records are properly secured when a health information custodian ceases to practice and that those records are available to patients on request.



Significant progress has been made in bringing institutions that are primarily funded by public dollars under Ontario's *Freedom of Information and*

Protection of Privacy Act (*FIPPA*) for the purposes of transparency and accountability, but further action is still needed.

In my 2004 Annual Report, I cited *universities*, *hospitals* and *Children's Aid Societies* as three large organizations that should be brought under this legislation. Since then, universities were made subject to the legislation in 2006, and the Ontario Hospital Association — to its great credit — voluntarily stepped forward in late 2009 and asked to have hospitals made subject to the law.

There have been some other progressive steps, including the two largest elements of what had been Ontario Hydro, being put back under *FIPPA*.

I urge the government to move quickly to bring hospitals under *FIPPA*. Once this is completed, the next step should be adding Children's Aid Societies, which are significantly funded by taxpayer dollars. In Alberta and Quebec, CASs are already covered under FOI legislation.

The Smart Grid will bring many benefits, including curbing greenhouse gas emissions and reducing consumers' energy bills. But consumer privacy is a crucial element that must be embedded in the electricity reform framework in Ontario.

I am very pleased with the response that my office has received since November when I first drew attention to this issue through a white paper — *Smart Privacy for the Smart Grid: Embedding Privacy in the Design of Electricity Conservation*. I have met with many stakeholders in the Ontario electrical sector and am happy to see a high level of understanding and commitment to privacy. In moving forward with plans in this area, the government must play a leadership role in ensuring that privacy forms a key part of the ongoing Smart Grid implementation in Ontario.

The infrastructure supporting the Smart Grid will be capable of informing consumers of their hourly and real-time energy use, and in the future at the individual appliance level. The overarching privacy concern I have raised is that there will be a great increase in the amount of information available relating to the activities of individuals within their homes — their habits and behaviours. In a future Smart Grid scenario that does not build in privacy, intimate details of hydro customers' lives could be easily discerned by data automatically fed by appliances and other devices to the companies providing electric power (e.g. what time you cook, shower, or go to bed — and the security issues such as whether the house has an alarm system).

Once inferences can be drawn on granular energy consumption information flowing outside of the home, such as real-time energy use data, future consumers may have questions including: *Who will have access to this sensitive data? For what purposes? What are the obligations of companies making smart appliances and Smart Grid systems to protect my privacy?* The best response is to ensure that privacy is proactively embedded into the design of the future Smart Grid, from start to finish – end to end. This is what I call *Privacy by Design*.

As we move forward, the Government of Ontario — in leading the province towards full Smart Grid implementation — must continue to ensure that privacy is a cornerstone of the Smart Grid.

Requests by the Public

2009 FOI Requests, by Jurisdiction and Records Type

	Personal Information	General Records	Total
Municipal	10,895	12,172	23,067
Provincial	3,783	10,240	14,023
Total	**14,678**	**22,412**	**37,090**

For the second year in a row, the number of freedom of information requests filed across Ontario has dropped, though the 37,090 FOI requests filed in 2009 is the third highest ever, following only 2007 and 2008.

One reason for the drop of 843 requests from 2008 was a positive disclosure development by the City of Toronto, which successfully diverted what would have been an additional 2,281 FOI requests (related to building plans) to its **expanded routine disclosure program.** Thus Toronto's 2009 total for FOI requests — 2,104 — is way below its 2008 total of 4,595.

Provincial government organizations received 14,023 FOI requests in 2009, an increase of more than four per cent from 2008's 13,451. Of the requests filed in 2009, 3,783 (roughly 27 per cent) were for personal information and 10,240 (73 per cent) were for general records.

The Ministry of the Environment continues to receive the largest number of requests under the provincial *Act* — 4,944 in 2009, though that number represents a decline of 312 from 2008. Once again, the ministries of Community Safety and Correctional Services (3,740), Community and Social Services (794), and Labour (616) were also among the ministries receiving the most requests. These four ministries received nearly three-quarters (72 per cent) of all provincial requests in 2009.

Municipal government organizations received 23,067 requests in 2009, a 5.8 per cent drop from the 24,482 requests received in 2008. (Outside the City of Toronto, municipal requests actually climbed from 19,887 in 2008 to 20,963 in 2009.) Of the 2009 requests, 10,895 (approximately 47 per cent) were for personal information and 12,172 (about 53 per cent) were for general records.

Police services boards received by far the most requests under the municipal *Act* — 14,183 (or about 61.5 per cent). Municipal corporations were next with 8,482 (nearly 37 per cent), followed by school boards with 205 requests (slightly under one per cent) and health boards with 77 requests (a third of one per cent).

And a very welcome trend continued in 2009 — of lower average fees for general records at the provincial level, which have consistently been much higher than other request fees.

See full statistics on 2009 FOI requests at www.ipc.on.ca

Average Cost of *Provincial* Requests	2006	2007	2008	2009
Personal Information	$11.55	$10.54	$11.26	**$ 9.47**
General Records	$51.11	$50.54	$42.74	**$39.66**

Average Cost of *Municipal* Requests	2006	2007	2008	2009
Personal Information	$ 8.64	$ 9.67	$ 8.82	**$ 8.11**
General Records	$21.04	$23.49	$23.54	**$26.55**

Response Rate Compliance

Response Rate Compliance: Top 10 Provincial Institutions

Ranked by the number of requests completed in 2009	Requests Received	Requests Completed	Within 30 Days	%	Extended Compliance *	Over 90 Days	%
Environment	4,944	4,830	3,975	82.3	97.7%	110	2.3
Community Safety and Correctional Services	3,740	3,784	2,884	76.2	96.4%	138	3.6
Community and Social Services	794	746	592	79.4	97.7%	17	2.3
Labour	616	640	572	89.4	95.0%	32	5.0
Attorney General	436	378	338	89.4	97.9%	8	2.1
Transportation	290	289	272	94.1	100.0%	0	0.0
Archives of Ontario	295	270	239	88.5	98.9%	3	1.1
Health and Long-Term Care	283	217	95	43.8	86.2%	30	13.8
Natural Resources	191	185	142	76.8	97.3%	5	2.7
Government Services	169	178	156	87.6	100.0%	0	0.0

*Including Notice of Extension, section 27(1) and Notice to Affected Persons, section 28(1). Such notices are used in circumstances where, for example, there is a need to search through a large number of records or consult with one or more people outside the organization.

Each year, to help focus attention on the importance of complying with the FOI response requirements set out in the *Acts*, the IPC reports compliance rates for each ministry and other government organizations. Since the IPC began reporting the individual response rates in 1999, the provincial 30-day compliance rate has climbed from 42 per cent to more than 80 per cent.

However, while the timelines in which responses are completed are very important, this **alone** does not indicate the quality of FOI responses from public institutions. For example, an institution may respond in a timely way but deny access to what should be routinely-available information.

Institutions Governed Under Provincial *Act*

After setting a record 30-day compliance rate for two straight years, provincial ministries, agencies and other provincial institutions produced an overall 30-day compliance rate of 81 per cent in 2009, a drop of four per cent from 2008.

The overall provincial extended compliance rate for 2009 was 97.2 per cent — a provincial record. (Extended compliance rates — where institutions can respond later than 30 days because of qualified extenuating circumstances — have only been calculated since 2002.)

The chart above lists the 10 provincial ministries and agencies that completed the most FOI requests in 2009, led by the Ministry of Environment with 4,830 completed requests (82.3 per cent within 30 days and a 97.7 per cent extended compliance rate) and the Ministry of Community Safety and Correctional Services with 3,784 (76.2 per cent within 30 days and a 96.4 per cent extended compliance rate).

The Ministry of Health and Long-Term Care, with a 30-day response rate of just 43.8 per cent, was the only provincial organization among the top 10 with a 30-day response rate below 76 per cent. Its extended compliance rate was nearly twice as high, at 86.2 per cent.

Institutions Governed by the Municipal *Act*

Municipal government institutions once again beat their provincial counterparts in responding to FOI requests within the statutory 30-day period — doing so 85.6 per cent of the time. With notices, the 2009 local government response rate rises to a record 97.7 per cent.

Toronto Police Services, which replaced the City of Toronto in 2009 as the local government organization that completed the most FOI requests (3,739) had a 30-day compliance rate of 76.9 per cent (94.4 per cent extended). The City of Toronto, which completed 2,072 requests, had a 30-day 77.5 per cent compliance rate (94.1 per cent extended), followed by Peel Regional Police, which completed 1,413 requests with an outstanding 30-day 100 per cent record.

See response rates for ministries, municipalities, police forces, school boards, etc., at www.ipc.on.ca

Appeals

Summary of Appeals: 2009 vs. 2008

2009	General Records			Personal Information			Total		
	Provincial	Municipal	**Total**	Provincial	Municipal	Total	Provincial	Municipal	**Total**
Opened	367	280	**647**	164	189	353	531	469	**1,000**
Closed	385	302	**687**	151	178	329	536	480	**1,016**

2008	General Records			Personal Information			Total		
	Provincial	Municipal	**Total**	Provincial	Municipal	Total	Provincial	Municipal	**Total**
Opened	261	316	**577**	148	194	342	409	510	**919**
Closed	260	302	**562**	181	223	404	441	525	**966**

Anyone who makes a written freedom of information request under Ontario's provincial or municipal *Freedom of Information and Protection of Privacy Act* and is not satisfied with the response has a right to appeal that decision to the IPC.

The *Acts* provide that, subject to limited and specific exemptions, information under the control of provincial and local government organizations should be available to the public.

Appeals may relate to a refusal to provide access, fees sought, the fact that the provincial or local government organization did not respond within the prescribed 30-day period, refusal to correct your personal information, or other procedural aspects relating to a request.

When an appeal is received, the IPC first attempts to settle it informally. If all issues cannot be resolved, the IPC may conduct an inquiry and issue a binding order, which may require the government organization to release all or part of the requested information.

Statistical Overview

In 2009, exactly 1,000 *personal information* and *general information* appeals were submitted to the IPC — the most in 14 years. The 2009 total is up nearly nine per cent from 2008. Overall, 1016 appeals were **closed** in 2009, the most in 13 years. The year-to-year increase from 2008 was slightly over five per cent.

Records that do not contain the personal information of the requester are referred to as general records. Overall, 647 appeals regarding access to *general records* were made to the IPC in 2009. Of these, 367 were filed under the provincial *Act* and 280 under the municipal *Act*, with the provincial number representing a major increase of nearly 41 per cent, and the municipal number down 11 per cent.

There were 353 *personal information* appeals filed to the IPC in 2009, including 164 under the provincial *Act* and 189 under the municipal *Act*. The provincial numbers were up by 16 and the municipal numbers down by five from the previous year.

Of the 531 appeals filed under the provincial *Act* with the IPC, 140 involved the Ministry of Community Safety and Correctional Services. The Ministry of Health and Long-Term Care was involved in 52, followed by the ministries of Community and Social Services (34) and Attorney General (30), the University of Ottawa (29), Ontario Lottery and Gaming Corporation (20), and the ministries of Environment (14), Natural Resources (14) and Finance (13).

And, of the 469 appeals received under the municipal *Act*, 235 (50 per cent) involved municipalities and another 185 (almost 40 per cent) involved police services.

Toronto Police Services and the City of Toronto, which again received more requests under the *Municipal Freedom of Information and Protection of Privacy Act* than any other government organization, also were involved in the most appeals under that *Act* — Toronto Police, 57; City of Toronto, 54, followed by the City of Vaughan (35), Ottawa Police (19), Halton Regional Police (18) and the City of Ottawa (17).

See full statistical information on appeals filed and how they were resolved at ***www.ipc.on.ca***

Privacy

Summary of Privacy Complaints: 2009 vs. 2008

	2008 Privacy Complaints				2009 Privacy Complaints			
	Provincial	Municipal	Non-jurisdictional	**Total**	Provincial	Municipal	Non-jurisdictional	**Total**
Opened	100	120	3	**223**	120	144	0	**264**
Closed	110	119	3	**232**	101	126	0	**227**

Ontario's provincial and municipal *Freedom of Information and Protection of Privacy Acts* establish rules that govern the collection, retention, use, disclosure, security, and disposal of personal information held by government organizations.

If you believe that your privacy has been compromised by a provincial or local government organization, you can file a complaint under the *Acts* with the IPC. In the majority of cases, the IPC attempts to mediate a solution. The IPC may also make formal recommendations to a government organization to amend its practices.

Privacy Complaints

There were 264 privacy complaints **opened** under the two public sector *Acts* in 2009 — the highest ever since the first of these *Acts* — the *Freedom of Information and Protection of Privacy Act* — came into effect in 1988. This represents an increase of 41 complaints (18 per cent) from 2008, when 223 privacy complaint files were opened.

Of the privacy complaints filed in 2009, 120 (roughly 45 per cent) were filed under the provincial *Act* and 144 (nearly 55 per cent) under the municipal *Act*. The increase in privacy complaints breaks down this way: 20 more complaints were filed under the provincial *Act* and 24 more under the municipal *Act* than the previous year.

When *collection, use or disclosure privacy complaints* under Ontario's *Personal Health Information Protection Act* are added to the privacy complaints filed under the public sector *Acts*, the number of privacy complaints filed with the IPC in 2009 jumps to 433.

Overall, 227 privacy complaints under the public sector *Acts* were **closed** in 2009. (When *collection, use or disclosure complaints* closed under *PHIPA* are added to those closed under the public sector *Acts*, the number closed climbs to 401.)

The disclosure of personal information was raised as an issue in 132 (58 per cent) of the complaints closed under the two public sector *Acts*. Another 25 (about 11 per cent) were related to security, while collection was an issue in 16 cases (nearly eight per cent). The remaining complaints involved such issues as use, retention, notice of collection and disposal.

The IPC continues to emphasize informal resolution and 222 of the 227 privacy complaints closed in 2009 were closed without the issuance of a formal privacy complaint report or order.

Of the complaints closed, 123 (about 54 per cent) had been initiated by individual members of the public, while 17 (seven per cent) were Commissioner-initiated. Eighty-seven (about 38 per cent) were self-reported breaches.

See more statistics on privacy complaints filed with the IPC in 2009 at www.ipc.on.ca

The *Personal Health Information Protection Act (PHIPA)*

The number of complaints filed with the IPC under the *Personal Health Information Protection Act (PHIPA)* dropped to 248 in 2009, a decrease of nearly 13 per cent from the 284 complaints filed in 2008.

It was the second straight year the number of complaints fell significantly. The number of complaints filed with the IPC climbed in the second and third full year of *PHIPA* (in 2006 and 2007) and then declined in 2008 and 2009.

With fewer complaints received in 2009, the number of complaint files closed by the IPC also dropped — to 240 from 302 in 2008.

Of the 2009 complaints, 79 were related to access or correction, while the other 169 were about the collection, use or disclosure of personal health information. Of the latter number, 101 were self-reported breaches. Commissioner Cavoukian strongly encourages health information custodians to quickly advise the IPC of any such breaches so the IPC can assist the custodian with taking quick steps to deal with the breach.

While 80 of the 248 complaints, about 32 per cent, were against public hospitals, this percentage continues to decrease — from 38 per cent in 2008 and 43 per cent in 2007. There were 28 complaints involving community or mental health centres, programs or services — up from 24 the previous year — while the number of complaints opened involving doctors dropped to 26 from 41. There were 17 complaints involving clinics (down from 24); 14 against Community Care Access Centres (up from seven) and 13 involving laboratories (up from eight).

At the individual health information custodian level, the Ministry of Health and Long-Term Care once again received, by far, the most requests from individuals for access to their own personal health information — a total of 3,123 requests, compared to 3,023 in 2008 and 2,450 in 2007.

Only health information custodians who also fall under *FIPPA* or *MFIPPA* are required to report such information to the IPC. The Ministry of Health and Long-Term Care traditionally receives about 85 per cent of the requests that are reported to the IPC.

The status of one of the key health groups in the province — general hospitals — may soon be changing. The Ontario Hospital Association requested late in 2009 that general hospitals be designated as institutions covered by the *Freedom*

(continued over page)

Fee Structure Needed

Since the ***Personal Health Information Protection Act*** came into force more than five years ago, the IPC has investigated numerous complaints about the fees charged by some health information custodians and their agents when clients ask for copies of their own personal health information.

PHIPA provides that the fee charged by a health information custodian for making such a record available to an individual ***shall not exceed the amount set out in the regulation under PHIPA, or the amount of reasonable cost recovery, if no amount is provided for in the regulation.*** To date, no such fee regulation has been passed.

In 2009, in response to a notice of proposed regulation published in the ***Ontario Gazette***, the IPC recommended to the Ministry of Health and Long-Term Care that Regulation 329/04 of ***PHIPA*** be amended to prescribe the fees that may be charged by health information custodians and their agents when disclosing personal health information or in providing access to a record of personal health information to the individual to whom the record relates.

Commissioner Cavoukian has emphasized that an amendment is needed in order to introduce uniformity and consistency across the health sector and in order to remove barriers experienced by individuals in seeking access to their own records of personal health information.

Type of *PHIPA* Complaint Files Opened in 2009

			Collection/Use/Disclosure							
	Access/ Correction	%	Individual	%	Self-reported Breach	%	IPC-initiated	%	Total	%
Public Hospital	32	40.5	20	36.4	25	24.8	3	23.1	80	32.3
Community or Mental Health centre, program	7	8.9	8	14.5	13	12.9	0	0.0	28	11.3
Doctor	12	15.2	6	10.9	8	7.9	0	0.0	26	10.5
Clinic	3	3.8	5	9.1	8	7.9	1	7.7	17	6.9
Community Care Access Centre	0	0.0	0	0.0	12	11.9	2	15.4	14	5.6
Laboratory	0	0.0	0	0.0	10	9.9	3	23.1	13	5.2
Other Health Professional	2	2.5	3	5.5	7	6.9	1	7.7	13	5.2
Dentist	2	2.5	2	3.6	2	2.0	1	7.7	7	2.8
Ministry of Health	3	3.8	1	1.8	2	2.0	1	7.7	7	2.8
Pharmacy	0	0.0	4	7.3	2	2.0	0	0.0	6	2.4
Independent Health Facility	2	2.5	1	1.8	2	2.0	0	0.0	5	2.0
Nursing Home	5	6.3	0	0.0	0	0.0	0	0.0	5	2.0
Other Prescribed Person	2	2.5	1	1.8	0	0.0	0	0.0	3	1.2
Pharmacist	1	1.3	0	0.0	1	1.0	1	7.7	3	1.2
Agent	1	1.3	0	0.0	1	1.0	0	0.0	2	0.8
Board of Health	0	0.0	1	1.8	1	1.0	0	0.0	2	0.8
Minister of Health	2	2.5	0	0.0	0	0.0	0	0.0	2	0.8
Physiotherapist	1	1.3	0	0.0	1	1.0	0	0.0	2	0.8
Social Worker	2	2.5	0	0.0	0	0.0	0	0.0	2	0.8
Other	2	0.0	3	1.8	6	0.0	0	0.0	11	0.4
Total	**79**	**100.0**	**55**	**100.0**	**101**	**100.0**	**13**	**100.0**	**248**	**100.0**

of Information and Protection of Privacy Act. This requested step, for which they have been praised by Commissioner Cavoukian, would leave hospitals responding to freedom of information requests for general information. It would also move them into the category of institutions that are covered by both *PHIPA* and *FIPPA* that report annually to the IPC on the number of requests they receive under *PHIPA* from individuals seeking access to their own personal health information.

See a full report of developments related to PHIPA *in 2009 at www.ipc.on.ca*

Judicial Reviews

The Ontario courts issued a number of key decisions in 2009 affirming the importance of the principle of transparency as embodied in Ontario's freedom of information legislation.

Among the court cases was one involving allegations of racial profiling by Toronto Police. The Court of Appeal upheld the IPC's decision that two databases held by the police qualified as "records" under the *Municipal Freedom of Information and Protection of Privacy Act*.

The requester, a journalist, had sought access to databases that contained information about individuals with whom the police had come into contact in the course of their duties. To avoid infringing on privacy rights, the journalist asked that the unique identifiers for each individual be replaced with randomly generated, unique numbers. The police refused the request on the basis that the information did not constitute a "record" under section 2(1) of *MFIPPA*, since the police would need to create new software to extract it.

After the requester appealed that decision to the IPC, the IPC ruled that the information did constitute a "record" under *MFIPPA*, and ordered the police to issue an access decision. On judicial review, the Divisional Court reversed the IPC's decision. The IPC appealed the Divisional Court's judgment to the Court of Appeal — Ontario's highest court.

The Court of Appeal upheld the IPC's decision, finding that unique numbers already exist within the database, and that replacing them with random numbers does not constitute "creating a new record." The Court of Appeal held that the police were able to create new software to respond to the request through technical expertise they normally use, and that the cost of doing so is a separate issue. Significantly, the Court of Appeal said that, when interpreting a freedom of information statute, it is vital to consider that governments "function to serve the public" and should be "open to public scrutiny." Further, the Court of Appeal said that any analysis of this type of issue must take into account the "prevalence of computers in society," and that "technological reality" suggests an interpretation of *MFIPPA* that would maximize rather than minimize the public's right of access to electronically-recorded information.

2009 Judicial Review Statistics

New Judicial Review applications received in 2009:

Launched by:	
Institutions:[1]	13
Requesters:[2]	1
Affected Parties:[3]	1
Total	**15**

Outstanding Judicial Reviews as of December 31, 2009:

Launched by:	
Institutions:	18
Requesters:	1
Institution and other Party:	4
Affected Parties:	7
Total	**30**

Judicial Reviews Closed/Heard in 2009:

Abandoned (Order Stands):[4]	4
Heard but Not Closed (decision pending):[5]	1
IPC Order Upheld:[6]	4
IPC Order Upheld (motion for leave to appeal pending):[7]	1
IPC Order Not Upheld (appeal pending):[8]	2
Total	**12**

1 PO-2739, PA08-92 (production order), PO-2762, PO-2775, MO-2408, MO-2425-I, PO-2793, PO-2807, PO-2811, MO-2416 and MO-2449, MO-2474, MO-2481
2 MO-2370
3 PO-2763
4 PO-2601-I, PO-2694, PO-2762, MO-2199
5 PA08-92 (production order)
6 MO-1989, PO-2494 and PO-2532-R, PO-2498
7 PO-2456
8 PO-2405 and PO-2538-R

See summaries of additional key Court rulings at www.ipc.on.ca

Financial Statement

	2009-2010 Estimates $	2008-2009 Estimates $	2008-2009 Actual $
Salaries and Wages	9,414,000	9,359,000	8,614,283
Employee Benefits	2,165,200	2,105,800	1,605,439
Transportation and Communications	296,000	345,000	325,490
Services	1,812,300	1,699,800	2,157,737
Supplies and Equipment	194,000	257,500	339,740
Total	**13,881,500**	**13,767,100**	**13,042,689**

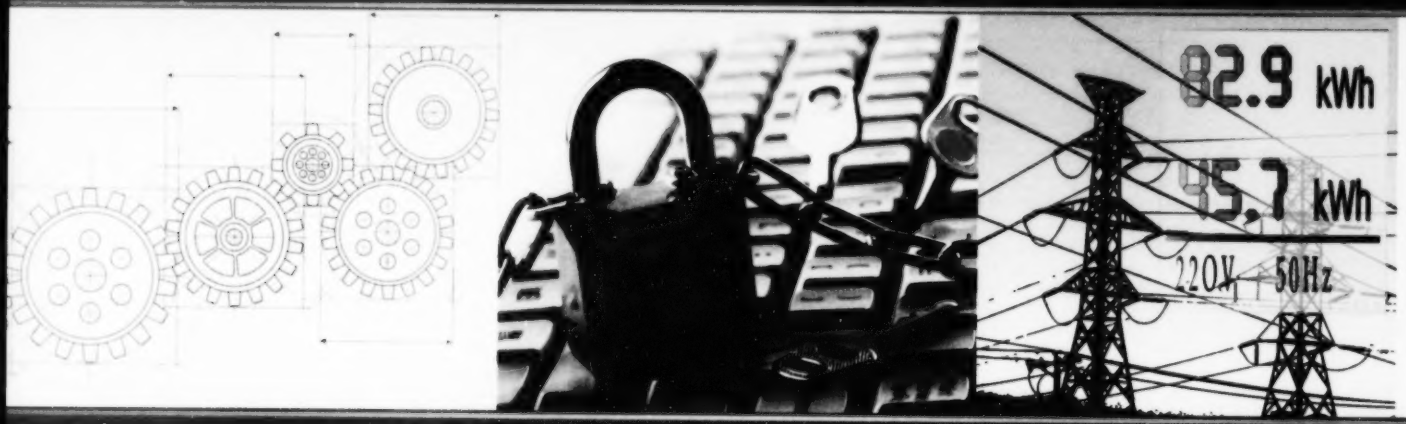
Note: The IPC's fiscal year begins April 1 and ends March 31.
The financial statement of the IPC is audited on an annual basis by the Office of the Auditor General of Ontario.

2009 Appeals Fees Deposit

(Calendar year)

General Info.	Personal Info.	Total
$11,597	$2,807	**$14,404**

See further financial information, including IPC Public Sector Salary Disclosure, at ***www.ipc.on.ca***



Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8
Canada

Tel: 416-326-3333
Fax: 416-325-9195
1-800-387-0073
TTY: 416-325-7539

E-mail: info@ipc.on.ca
Web: www.ipc.on.ca